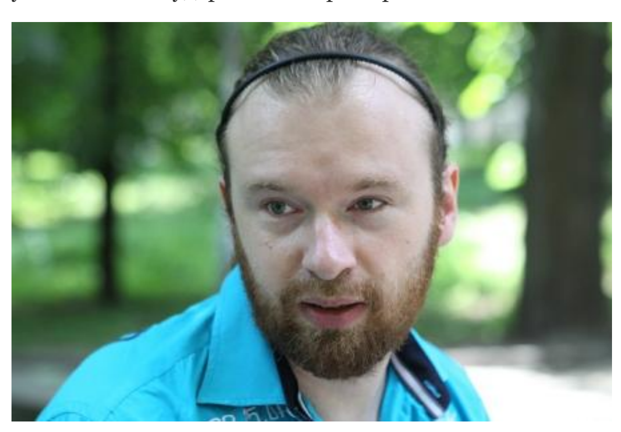
Глеб Пахаренко: под угрозой все, что можно быстро монетизировать

Эксперт по кибернетической безопасности Глеб Пахаренко в эксклюзивном интервью рассказал Контрактам об угрозе хакерских атак, беспорядке в IT системах банков и уязвимости государственных реестров.

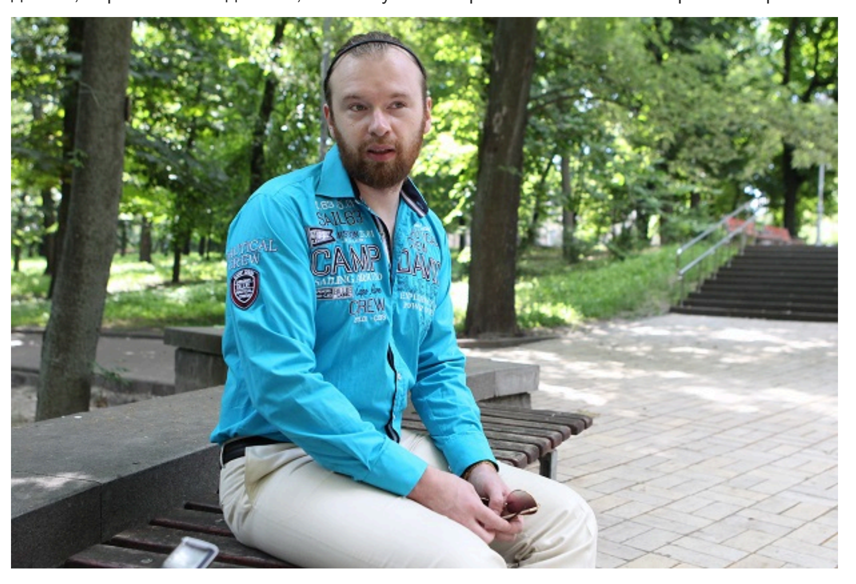


Не так давно в социальных сетях появилась информация, что на просторах СНГ, в то числе и в Украине активно орудуют международные хакерские преступные группировки Carbanak / Akunak и Buhtrap, которые создали и разместили в открытом доступе набор инструментов для проникновения в банки и другие финансовые учреждения. На данный момент благодаря действиям этих группировок уже скомпрометировано десятки банков в странах бывшего Союза, из которых украдено сотни миллионов долларов. О том, чем угрожают атаки международных хакеров украинским финансовым учреждениям, и способен ли банковский сектор им противостоять Контракты расспросили у эксперта по кибернетической безопасности, директора компании Pakurity Глеба Пахаренко. А заодно поговорили с ним о мошенничестве внутри коммерческих структур, манипуляциях с электронными базами данных и уязвимости информационных систем государственных органов.

К: Глеб, какие отрасли или структуры в Украине более всего подвергаются хакерским атакам и почему?

Глеб Пахаренко: Больше всего атакуют финансовые учреждения, медиа-сектор, энергетику и государственные учреждения. В банки вторгаются, чтобы получить финансовую выгоду. СМИ атакуют на заказ и для поддержки информационных войн. А вот атаку последних двух секторов чаще всего заказывают спецслужбы других стран или кибер-преступники, которым нужен доступ к госреестрам.

Но кроме этого, атакам хакеров подвержены и обычные пользователи. У них, например, воруют деньги, персональные данные, используют их персональные компьютеры в хакерских операциях.



К: На сегодняшний день существует какая-то классификация хакеров?

Глеб Пахаренко: Да, сегодня выделяют несколько видов хакеров, хотя все эти границы очень условны. В Украине, например, мы чаще всего встречаемся с сотрудниками спецслужб, которые используют так называемые методы преодоления логической защиты для проникновения в системы; профессиональными киберпреступниками, которых довольно часто привлекают те же спецслужбы. К слову, в среде киберпреступников существует целая иерархия: одни из них разрабатывают вирусы, другие заражают ими компьютеры, третьи используют зараженные

компьютеры для распространения спама, четвертые воруют деньги пользователей интернет-банков. Некоторые же киберпреступники даже атакуют сами банки.

Кроме того, среди хакеров, которые орудуют в Украине, нужно вспомнить и «случайных» IT-шников, учеников средних и высших учебных заведений, хактивистов, а также профессиональных специалистов по безопасности, которые по тем или иным причинам решают проникнуть без разрешения в другие сети.

Наиболее популярные атаки, которые применяются в нашей стране – это DDos-атаки - хакерская атака на вычислительную систему с целью довести её до отказа; приложения Locker, которое обходит локальные/сетевые диски и шифрует все пользовательские файлы, а также разные виды троянских коней, которые используются с целью захвата ПК и его контроля, а также воровства данных.



К: А чем именно опасны действия группировок, подобных Carbanak / Akunak и Buhtrap? Говорят, что атаки, которым подвергаются финансовые учреждения со стороны этих злоумышленников, намного серьезнее, чем атаки обычных хакеров.

Глеба Пахаренко: Хакеры подобного рода в первую очередь атакуют платежные сервисы: СЭП, процессинг, интернет-банкинг, банкоматы, системы денежных переводов и т.д. Самый известный случай, когда подобного рода злоумышленники украли деньги со счетов правительства Бангладеша в Нью-Йорской федеральной системе. Хакерам удалось украсть $86 млн. Точнее, это та сумма, которую банкам не удалось вернуть. На самом же деле переводы были сделаны на сотни миллионов долларов.

То есть, речь идет о хакерах, которые не просто взламывают сервер, рассылают с помощью него спам и забывают о нем. Это злоумышленники, которые после проникновения в банк изучают его работу и внутренние процессы несколько месяцев. После чего они используют полномочия легитимных пользователей для создания платежей через международную межбанковскую систему платежей и систему электронных платежей СЭП, и также атакуют банкоматы и карточный процессинг.

К: Неужели банки, в которых хакеры работают несколько месяцев, не могут обнаружить, что их атакуют?

Глеб Пахаренко:Особенность этих группировок в том, что там работают профессионалы высокого класса. Перед тем, как «хакнуть» банк они делают тесты на проникновение, точно та к, как аудиторы безопасности, когда воспроизводят действия хакеров и пытаются проникнуть в компанию, с целью предоставления отчетов, как они это сделали. Такое чувство, что некоторые из злоумышленников раньше работали как «белые» хакеры, то есть, в аудите безопасности: они знают, как работаю платежные системы, разбираются в базах данных. Я даже могу догадываться, что среди них есть человек, который ранее работал в банковской системе. Кроме того, чтобы вывести миллионы, нужно иметь людей, которым ты доверяешь, которые не украдут эти деньги сами. То есть, это мощные группировки и противостоять им крайне сложно.



К: А банковское сообщество может решить эту проблему как-то сообща. Как финансовые учреждения защищают себя, например, в той же Европе?

Глеб Пахаренко: В идеале, если взломали один банк, то все остальные учреждения должны получить соответствующие IP адреса, информацию о вирусе, их признаках и просканировать свои системы. Кроме того, в регулирование этого вопроса может вмешаться и государство. Как, например, сделали в Австрии? У них регулятор потребовал от банков создать команду реагирования на инциденты. Но эта команда не предоставляет регулятору ничего, кроме статистики. Таким образом, центральный банк не может ополчиться на пострадавший банк и обвинить его в непрофессионализме или еще чем-то. То есть, если банк взломали, то регулятор узнает об этом только в конце года из общих данных о том, сколько банков взломано всего и на какую сумму. Поэтому банки доверяют этой команде.

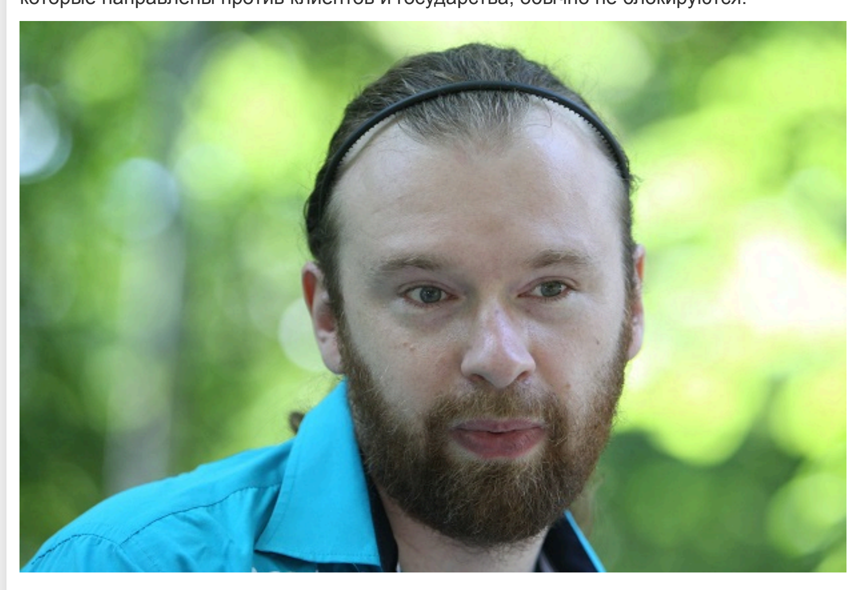
К: Глеб, скажите, а сами сотрудники банков могут умышленно заниматься мошенничеством благодаря все большей автоматизации банковской системы, например, подтасовывать базы данных, воровать деньги у клиентов? У меня был случай, когда наша читательница выставила банку претензии именно в подтасовывании информации в базе данных.

Глеб Пахаренко: Во многих банках полный беспорядок в IT, поэтому в них действительно может быть большое количество мошенничества, при чем с привлечением разного уровня сотрудников.

К: Насколько успешно банки ведут борьбу с такими случаями?

Глеб Пахаренко: Они ведут борьбу только, если мошенничество несет им существенные прямые убытки. Если внедрения мероприятий по предотвращению мошенничества слишком дорого, а потери несут только некоторые клиенты, а не банк, тогда ничего не делается.

Вообще в банках есть отделы антифроду, но они больше борются с мошенничеством со стороны клиентов (оплата проблемных кредитов) или, в лучшем случае, с мошенничеством операционистов и кассиров. Все остальные виды мошенничества, в которых замешено руководство банка, и которые направлены против клиентов и государства, обычно не блокируются.



К: А какие бывают виды мошенничества с помощью информационных технологий в государственных органах? Ведь не только частный сектор грешит подобного рода делами?

Глеб Пахаренко: В государственных органах, в силу высокого уровня коррупции, мошенничество достигает огромных объемов. Вспомните только экзамены в ГАИ! Там, если не заплатил, то сдать их

очень трудно. А если заплатил, то, какие бы ответы человек не вбивал в компьютер, в итоге он получает хороший результат. Это очень известный факт, и никто в государстве с этим не борется.

Если же говорить об уязвимости баз данных или госреестров, то достаточно вспомнить недавний случай, когда молодой специалист из Одессы нашел брешь в реестре земельных участков и скачал из него все данные. Уверен, что в других системах также есть куча дыр, через которые хакеры могут производить любые изменения.

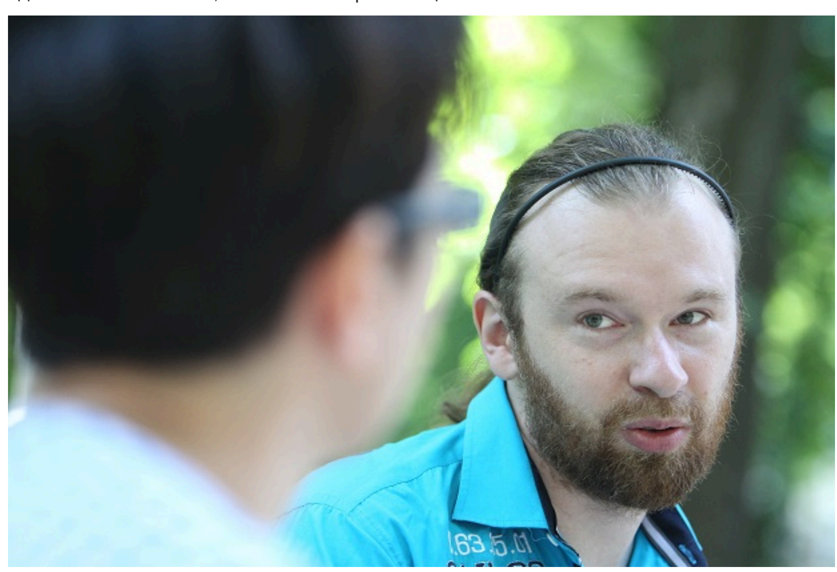
К: Но как же система контролей, встроенных в IT системы? Неужели их так просто обойти?

Глеб Пахаренко: К сожалению, наши госорганы делают это постоянно. Например, система ставит плохие отметки на экзамене, и распечатывает ведомость, что кто-то не сдал экзамен на такую-то должность. Комиссия принимает эти результаты, а потом от руки заполняет пустой бланк и вносит туда те отметки, которые захочет. При этом систему никто не проверяет. А системный администратор может затем затереть журналы или вообще что-то дописать в систему, чтобы она сразу ставила хорошие отметки тем кому нужно.

Вообще, отмечу, что IT контроли сами по себе предотвращают только до 10% мошенничества. Все остальное - это организационные меры, привлечение к процессу контроля независимых сторон, максимальная прозрачность и ведение учета действий.

Также важно участие в процессе контроля всех участников процесса, которые извещали бы общественность о нарушениях. Ведь, как утверждают международные исследования, своевременное оповещение раскрывает до 70% случаев мошенничества.

И еще важный момент – внедрение системы безопасности требует изменения культуры организации, включая рядовых сотрудников и топ-менеджмеров. А это, как известно, очень тяжело сделать в постоянных, неизменных организациях.



К: Информационные системы госорганов действительно интересны профессиональным хакерам, как вы упоминали в начале интервью?

Глеб Пахаренко: Не так давно было была статья о том, что хакеры взломали реестры нотариусов. Теперь у них есть ключи доступа к разным реестрам.

На самом деле, под угрозой все то, что можно быстро монетизировать. Есть хакеры политически мотивированные, есть те, которые работают на спецслужбы иностранных государств, службы внешней разведки, полицию. В одном учреждении может сидеть несколько хакерских групп и исполнять совершенно разные задачи.

Автор: Елена Романюк

Комментарии: 0

Сортировка **Сначала старые**



Добавьте комментарий...

Плагин комментариев Facebook